REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application. Claims 22-77 are canceled without prejudice; Applicant reserves the right to pursue claims 22-77 in one or more continuation applications. Claims 1-21 are pending in this application.

35 U.S.C. § 103

Claims 1-5, 7, 9-13, 15, and 17-19 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,944,821 to Angelo (hereinafter "Angelo") in view of Arbaugh. Applicant respectfully submits that claims 1-5, 7, 9-13, 15, and 17-19 are not obvious over Angelo in view of Arbaugh.

As discussed in the Abstract of Angelo, Angelo is directed to a method for providing secure registration and integrity assessment of software in a computer system. A secure hash table is created containing a list of secure programs that the user wants to validate prior to execution. The table contains a secure hash value (i.e., a value generated by modification detection code) for each of these programs as originally installed on the computer system. This hash table is stored in protected memory that can only be accessed when the computer system is in system management mode. Following an attempt to execute a secured program, a system management interrupt is generated. An SMI handler then generates a current hash value for the program to be executed. In the event that the current hash value matches the stored hash value, the integrity of the program is guaranteed and it is loaded into memory and executed. If the two values do not

match, the user is alerted to the discrepancy and may be given the option to update or override the stored hash value by entering an administrative password.

Angelo, as discussed in section 1.1, 1st paragraph, is directed to a system referred to as AEGIS. AEGIS ensures the integrity of the bootstrap code by constructing a chain of integrity checks, beginning at power-on and continuing until the final transfer of control from the bootstrap components to the operating system itself. The integrity checks compare a computed cryptographic hash value with a stored digital signature associated with each component.

With respect to amended claim 1, amended claim 1 recites:

> In a computer system having a central processing unit (CPU) and an operating system (OS), the CPU having a software identity register, a method for booting the operating system comprising:
>
> computing a cryptographic function of at least a portion of the operating system; and
>
> setting the software identity register to a result of the computed cryptographic function if atomic execution of a boot block of the operating system does not fail, and otherwise setting the software identity register to a value indicating that the atomic execution of the boot block failed.

Applicant respectfully submits that Angelo in view of Arbaugh does not disclose or suggest such setting of a software identity register to one value if atomic execution of a boot block of the operating system does not fail, otherwise setting the software identity register to another value.

Applicant respectfully submits that there is no discussion or mention in either Angelo or Arbaugh of any such setting of a software identity register to one of two values as recited in amended claim 1. As there is no such discussion or mention in either Angelo or Arbaugh, Applicant respectfully submits that Angelo in view of Arbaugh cannot disclose or suggest the method of amended claim 1.

Applicant notes that in the February 9, 2005 Office Action at p. 6, in the rejection of claim 3, it was asserted with respect to Angelo that:

> The hash value can be deleted; this would be setting the value to something other than the correct hash value. The user is also given a choice to update the value and put in a value that is different from the correct hash value.

Applicant respectfully submits that deleting of hash value or updating a value as discussed in Angelo does not disclose or suggest otherwise setting the software identity register to a value indicating that the atomic execution of the boot block failed as recited in amended claim 1.

In Angelo, the system is configured to query the user to update the hash table and/or stored hash value to incorporate the program as it currently exists if no hash value corresponding to the program to be executed is found or if the stored hash value does not equal the newly calculated hash value (see, col. 10, lines 39-52). In addition to adding or updating entries for programs that the user wants to verify prior to execution, entries can be deleted for programs that are no longer utilized (see, col. 10, lines 61-64). However, there is no discussion or mention in this querying of the user or in this deletion of entries that a software identify register is set to a value indicating that atomic execution of a boot block failed as recited in amended claim 1. Without any such discussion or mention, Applicant respectfully submits that this querying of the user and this deletion of entries of Angelo does not disclose or suggest otherwise setting the software identity register to a value indicating that the atomic execution of the boot block failed as recited in amended claim 1.

For at least these reasons, Applicant respectfully submits that amended claim 1 is allowable over Angelo in view of Arbaugh.

Given that claim 2 depends from amended claim 1, Applicant respectfully submits that claim 2 is likewise allowable over Angelo in view of Arbaugh for at least the reasons discussed above with respect to amended claim 1.

With respect to amended claim 3, Applicant respectfully submits that, similar to the discussion above regarding amended claim 1, Angelo in view of Arbaugh does not disclose or suggest executing an atomic operation to set an identity of the operating system into the software identity register of the CPU, wherein in an event that the atomic operation completes correctly, the software identity register contains the identity of the operating system and in an event that the atomic operation fails to complete correctly, the software identity register contains a value indicating that the atomic operation failed as recited in amended claim 3. For at least these reasons, Applicant respectfully submits that amended claim 3 is allowable over Angelo in view of Arbaugh.

Given that claims 4-5 and 7 depend from amended claim 3, Applicant respectfully submits that claims 4-5 and 7 are likewise allowable over Angelo in view of Arbaugh for at least the reasons discussed above with respect to amended claim 3.

With respect to claim 9, claim 9 depends from amended claim 3 and Applicant respectfully submits that claim 9 is allowable over Angelo in view of Arbaugh for at least the reasons discussed above with respect to amended claim 3. Furthermore, claim 9 recites:

> The method as recited in claim 3, further comprising generating a storage key for encrypting data to be stored on the computer system from a seed based in part on the identity of the operating system.

Applicant respectfully submits that Angelo in view of Arbaugh does not disclose or suggest generating a storage key as recited in claim 9.

In the February 9, 2005 Office Action at p. 7, it was asserted that:

> *In reference to claims 4, 9, 10, 12, 17, and 18,* the identity comprises a public key of a correctly signed block of code from the operating system, and examining a content of the software identity register comprises verifying a signature of the signed block of code against the public key (Section 3.2.2 paragraph 2 Arbaugh).

This rejection of claim 9 does not make any reference to generating a storage key for encrypting data to be stored on the computer system from a seed based in part on the identity of the operating system or where such generating is asserted as being disclosed in Arbaugh or Angelo. Section 3.2.2 paragraph 2 of Arbaugh also does not include any discussion or mention of generating a storage key for encrypting data to be stored on the computer system from a seed based in part on the identity of the operating system as recited in claim 9. Without any such discussion or mention, Applicant respectfully submits that Arbaugh cannot disclose or suggest generating a key as recited in claim 9.

For at least these reasons, Applicant respectfully submits that claim 9 is allowable over Angelo in view of Arbaugh.

Given that claim 10 depends from claim 9, Applicant respectfully submits that claim 10 is likewise allowable over Angelo in view of Arbaugh for at least the reasons discussed above with respect to claim 9.

With respect to amended claim 11, Applicant respectfully submits that, similar to the discussion above regarding amended claim 1, Angelo in view of Arbaugh does not disclose or suggest executing an atomic operation to set the identity of the operating system into the software identity register of the CPU,

wherein in an event that the atomic operation completes correctly, the software identity register is set to contain the identity of the operating system, and in an event that the atomic operation does not complete correctly, the software identity register is set to contain a false value to indicate failure of the atomic operation as recited in amended claim 11. For at least these reasons, Applicant respectfully submits that amended claim 11 is allowable over Angelo in view of Arbaugh.

Given that claims 12-13 and 15 depend from amended claim 11, Applicant respectfully submits that claims 12-13 and 15 are likewise allowable over Angelo in view of Arbaugh for at least the reasons discussed above with respect to amended claim 11.

With respect to claim 17, claim 17 depends from amended claim 11 and Applicant respectfully submits that claim 17 is allowable over Angelo in view of Arbaugh for at least the reasons discussed above with respect to amended claim 11. Furthermore, Applicant respectfully submits that, similar to the discussion above regarding claim 9, Angelo in view of Arbaugh does not disclose or suggest generating a storage key for encrypting data to be stored on the computer system from a seed based in part on the identity of the OS as recited in claim 17. For at least these reasons, Applicant respectfully submits that claim 17 is allowable over Angelo in view of Arbaugh.

Given that claim 18 depends from claim 17, Applicant respectfully submits that claim 18 is likewise allowable over Angelo in view of Arbaugh for at least the reasons discussed above with respect to claim 17.

With respect to amended claim 19, amended claim 19 recites:

> In a computer system having a central processing unit (CPU) and an operating system (OS), the CPU having a pair of private and

public keys and a software identity register that holds an identity of the operating system, a method comprising:

creating an OS certificate including the identity from the software identity register, information describing the operating system, and the CPU public key; and

signing the OS certificate using the CPU private key.

Applicant respectfully submits that Angelo in view of Arbaugh does not disclose such creating and signing.

In the method of amended claim 19, an OS certificate is created that includes the identity from the software identity register, information describing the operating system, and the CPU public key. No such OS certificate is discussed or mentioned in Angelo or Arbaugh. Although Arbaugh may mention public key cryptography, there is no discussion or mention in Arbaugh of signing an OS certificate using a CPU private key where the OS certificate includes the identity from the software identity register, information describing the operating system, and the CPU public key. Accordingly, for at least these reasons Applicant respectfully submits that claim 19 is allowable over Angelo in view of Arbaugh.

Claims 6, 8, 14, 16, and 21 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Angelo in view of Arbaugh and further in view of U.S. Patent No. 6,230,285 to Sadowsky et al. (hereinafter "Sadowsky"). Applicant respectfully submits that claims 6, 8, 14, 16, and 21 are not obvious over Angelo in view of Arbaugh and further in view of Sadowsky.

As discussed in the Abstract of Sadowsky, Sadowsky is directed to a boot failure recovery system that operates to diagnose a failed system boot in a computer operating system which boots by bootstrapping from a boot sector of a storage medium using configuration information. The boot failure recovery system includes an agent which monitors operating system files used during

system boot and which stores information regarding changes to the system files to a change file. A repair module analyzes the change file to determine the cause of the failed system boot. A boot check module responds to initiation of a system boot by determining if a prior system boot was successful. The boot check module causes execution of a first boot sector code module upon occurrence of a successful prior system boot and causes execution of the repair module upon occurrence of a failed prior system boot.

With respect to claims 6 and 8, claims 6 and 8 depend from amended claim 3 and Applicant respectfully submits that claims 6 and 8 are allowable over Angelo in view of Arbaugh for at least the reasons discussed above with respect to amended claim 3. Sadowsky is not cited as curing, and does not cure, the deficiencies of Angelo in view of Arbaugh discussed above with respect to amended claim 3. Accordingly, for at least these reasons, Applicant respectfully submits that claims 6 and 8 are allowable over Angelo in view of Arbaugh and further in view of Sadowsky.

With respect to claims 14 and 16, claims 14 and 16 depend from amended claim 11 and Applicant respectfully submits that claims 14 and 16 are allowable over Angelo in view of Arbaugh for at least the reasons discussed above with respect to amended claim 11. Sadowsky is not cited as curing, and does not cure, the deficiencies of Angelo in view of Arbaugh discussed above with respect to amended claim 11. Accordingly, for at least these reasons, Applicant respectfully submits that claims 14 and 16 are allowable over Angelo in view of Arbaugh and further in view of Sadowsky.

With respect to claim 21, claim 21 depends from amended claim 19 and Applicant respectfully submits that claim 21 is allowable over Angelo in view of Arbaugh for at least the reasons discussed above with respect to amended claim 19. Sadowsky is not cited as curing, and does not cure, the deficiencies of Angelo in view of Arbaugh discussed above with respect to amended claim 19. Accordingly, for at least these reasons, Applicant respectfully submits that claim 21 is allowable over Angelo in view of Arbaugh and further in view of Sadowsky.

Claim 20 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Angelo in view of Arbaugh and further in view of U.S. Patent No. 6,026,166 to LeBourgeois et al. (hereinafter "LeBourgeois"). Applicant respectfully submits that claim 20 is not obvious over Angelo in view of Arbaugh and further in view of LeBourgeois.

As discussed in the Abstract of LeBourgeois, LeBourgeois is directed to a digital certification method in which a first digital signature dependent upon a first user identity and a first user system in combination, is stored accessibly to a certification server. The first user identity can be distinguished by, for example, a PIN provided by the user. Subsequently, the user system generates a second signature dependent upon both the current user identity and the current user system in combination. The certifying system then compares the second signature with the first, as stored, to certify the transaction. The certification can accommodate normal computer system component drift. An inquiring system, desiring to confirm the identity of a user, issues a challenge code to the user system. The user system then digests the user's PIN, individual component signatures as they currently exist on the user's system, together with the challenge

code to generate the new signature. The new signature is transmitted back to the inquiring system, which transmits it on to the certification server together with the challenge code. The certification server then digests the challenge code with the original signature as previously stored, and compares the result to the newly provided signature to confirm the users identity, else drift criteria can be applied if desired.

With respect to claim 20, claim 20 depends from amended claim 19 and Applicant respectfully submits that claim 20 is allowable over Angelo in view of Arbaugh for at least the reasons discussed above with respect to amended claim 19. LeBourgeois is not cited as curing, and does not cure, the deficiencies of Angelo in view of Arbaugh discussed above with respect to amended claim 19. Accordingly, for at least these reasons, Applicant respectfully submits that claim 20 is allowable over Angelo in view of Arbaugh and further in view of LeBourgeois.

With respect to claims 22-77, claims 22-77 have been canceled without prejudice, thereby rendering the rejection of claims 22-77 moot.

Applicant respectfully requests that the §103 rejections be withdrawn.

Conclusion

Claims 1-21 are in condition for allowance. Applicant respectfully requests reconsideration and issuance of the subject application. Should any matter in this case remain unresolved, the undersigned attorney respectfully requests a telephone conference with the Examiner to resolve any such outstanding matter.

Respectfully Submitted,

Date: 8/9/05

By: _____

Allan T. Sponseller
Reg. No. 38,318
(509) 324-9256